CHAPTER 1: POLICY DEFINED

Multiple Choice:

1. **Which of the following is NOT a state in which information exists?**

A. stored
B. processed
C. factored
D. transmitted

E. Why is it important to consistently enforce policy, and not "go easy on someone"?

F. The welfare of the overall organization is more important than the individual's

G. Playing favorites creates resentment

H. It is easier to defend in court

I. Policies should never be broken

J. Which of the following is LEAST likely to lead to employees accepting and following policy?

K. Introduce policies through training programs
L. Make policy compliance part of the job descriptions
M. Consistently enforce policies
N. Seek input from the organization when developing policies

O. Why is it important to prepare written policies?

P. So the policies can be communicated more easily
Q. This helps to ensure consistency
R. A policy is part of the corporate culture
S. It is required by law

T. Why is it important for leadership to set a tone of compliance with policy?

U. The rest of the organization feels better about following the rules

V. It is part of their job

W. Management are some of the worst offenders

X. They are the ones that write the policies

Y. When should information security policies, procedures, standards, and guidelines be revisited?

Z. As indicated in the policy

AA. Never; once they are written and published, they must be adhered to

BB. Annually

CC. When dictated by change drivers

DD. Which is the best way to foster acceptance of a new policy?

EE. Involve people in policy development by conducting interviews

FF. Give everyone a copy of the policy after it is written

GG. Ensure it is detailed enough that everyone will understand it

HH. Hold meetings to explain it

II. Which is a two wall challenge?

JJ. Screened-subnet firewall

KK. Requiring security badges at both doors to a room

LL. Lack of awareness, and the lack of awareness about the lack of awareness

MM. When two policies conflict with each other

NN. Which is the preferred approach to organizing information security policies, procedures, standards, and guidelines?

OO. Combine policies and procedures

PP. Keep the policy documents separate from the procedures, standards, and guidelines

QQ. Combine standards and guidelines

RR. Keep them all separate

SS. Why do we need the Graham-Leach-Bliley Act (GLBA)?

TT. The information banks possess can be identifiable and whole in regard to any customer

UU. It protects banks from lawsuits due to a lack of fair treatment of employees

VV. Health care organizations must safeguard private health care information from disclosure

WW. Businesses need expert advice to achieve and sustain compliance

XX. What should be the consequences of information security policy violations?

YY. Always up to, and including, termination

ZZ. Immediate revocation of all user privileges

AAA. Commensurate with the criticality of information the policy was written to protect

BBB. Violations should be cited in the person's annual performance review

CCC. Leadership by setting the example, or "do as I do", is considered:

DDD. Ineffective in a high-tech company

EEE. The same as "management by walking around"

FFF. Something that should only be employed when information security policies are new

GGG. The most effective leadership style, especially in relation to information security

HHH. Why is it important to remind people about best practice information security behaviors?

III. This approach is a mandatory requirement of information security policies

JJJ. Reminders are the least expensive way to ensure compliance with policies

KKK. It ensures they are aware that management is watching them

LLL. Reminders reinforce their knowledge, and help them better understand expectations

MMM. Which is the worst that may happen if information security policies are out of date, or address technologies no longer used in the organization?

NNN. People may take the policies less seriously, or dismiss them entirely

OOO. Executive management may become upset

PPP. The company may incur unnecessary costs to change them

QQQ. People may not know which policy applies

RRR. Which is the best goal for a new policy?

SSS. Accurately reflect the current technology environment

TTT. Comply with applicable government policy

UUU. Secure and protect assets from foreseeable harm, and provide flexibility for the unforeseen

VVV. Approved by management, and understood by everyone

WWW. **Which part of the U.S. Constitution is analogous to the first approved version of a new information security policy**?

XXX. amendments
YYY. articles
ZZZ. the Torah
AAAA. the Bill of Rights

BBBB. In what way are the Torah and the U.S. Constitution like information security policies?

CCCC. They contain articles and amendments

DDDD. They include business rules

EEEE. They define the role of government in our daily lives

FFFF. They serve as rules to guide behavior in support of organizational goals

GGGG. What issue is addressed by both the Bible and corporate policies?

HHHH. People tend to forget things if they are not periodically reminded of their obligations

IIII. Without common rules, people may adopt common behaviors and choices that make the overall group less stable

JJJJ. Stealing

KKKK. The behavior of people in power

Fill in the Blank:

LLLL. An information security _____ exists when users share account names and passwords with each other.

Answer: gap

MMMM. An organization which does not enforce policy is said to have _____ policies.

Answer: paper only

NNNN. The _____ are either elected or chosen to direct the affairs of a corporation, and are responsible for providing oversight of the information security program.

Answer: Board of Directors

OOOO. According to HIPAA, private health care information must remain protected from damage, misuse, and _____.

Answer: disclosure

The U.S. Constitution's _____ are the built-in framework that makes it possible to change the document, while still adhering to its original intent.

Answer: amendments

Matching:

PPPP. Match each role with its responsibilities to the right:

I.	Board of Directors	A. Ensure that information security controls are functioning as intended
II.	Information Owner	B. Approve written information security policies
III.	Data Custodian	C. Establish the controls that provide information security
IV.	ISO	D. Process and store information
V.	Internal Auditor	E. Administer the information security function

Answer: B C D E A

QQQQ. Match the following terms to their meanings:

I.	Foreign Policy	A. Policy adopted by society through legislative means to govern its people
II.	Law	B. Civil or criminal; imposed for violations
III.	Policy Area	C. A general topic, which relates to specific behavior and expectations
IV.	Penalty	D. Standards for public and private education
V.	Education Policy	E. Ways and means for one nation to deal with another

Answer: E A C B D

CHAPTER 2: THE ELEMENTS OF A POLICY

IT 409

Multiple Choice:

1- **What are the two schools of thought regarding policy format?**

RRRR. **A separate document for each policy, or one large document with multiple sections**

SSSS. Use Microsoft Word, or Adobe Acrobat

TTTT. The ISO approach, or the OSI approach

UUUU. One large document with multiple sections or one large document

2- **Where should the penalty for violating a policy be listed?**

a. In the first chapter of the Employee Handbook

b. **In the policy enforcement clause within the policy**

c. In the policy violation penalties document

d. In the policy enforcement document

3- **Which of the following are all federal regulations?**

a. Sarbanes-Oxley, IEEE 802.11, NIST 800-34

b. **GLBA, HIPAA, and Sarbanes-Oxley**

c. GLBA, HIPAA, and IEEE 802.11

d. GLBA, NIST 800-34, and Sarbanes-Oxley

4- **Which of the following is NOT a way in which the number of policy exceptions reflect on the quality of a policy?**

a. **Too many exceptions to a valid rule in a policy may mean that there is a loophole in the policy.**

b. Too many exceptions to a rule in a policy may mean that the rule is inappropriate.

c. Too many exceptions to a rule in a policy may mean that employees perceive the rule as unimportant.

d. Too many exceptions to a valid rule may cause employees to feel that favoritism is being extended to some, but not all, employees

5- **In what way is a speed limit like a standard?**

a. They are not alike at all

b. A standard, like a speed limit, is always expressed in numeric form

c. A speed limit, like a standard, is very definite, and required

d. Both are suggested levels of performance

6- Which of the following is the best example of an acceptable password?

a. T0yot@tRuck
b. May12345
c. FredD
d. HappyDeyz

7- Which of the following is an outline of a complete policy?

a. Purpose, Objectives, Policy, Exceptions, and Disciplinary Actions

b. Objectives, Purpose, Policy, Exceptions, and Disciplinary Actions

c. Objectives, Purpose, Audience, Policy, Exceptions, and Procedures

d. Objectives, Purpose, Audience, Policy, Exceptions, and Disciplinary Actions

8- Which of the following is a good rule of thumb for including definitions in a policy?

a. Always include a definitions section at the end of a policy

b. Include definitions for any instance of non-standard language

c. Provide the definition of any non-standard word in parentheses after the word's first appearance

d. Cite sources of information about non-standard terms in the policy's bibliography

9- Which of the following is the best definition of a policy audience?

a. All employees granted unescorted access to the company's computer room

b. All headquarters employees

c. Any employee in the computer room

d. Only those employees in the computer room

10- **Which of the following should you strive for in the policy statement, in order to have a well-written policy?**

a. **Contain areas that address every aspect of operations and information, and every area affecting the organization's information assets**

b. Spell check the document to avoid typographical errors

c. Include applicable standards, guidelines, and procedures within the policy document

d. Describe everything in layman's terms, so that it is clear the policy is a statement of everyone's intent

11- **Which of the following is true of procedures?**

a. **Procedures focus on sequential actions or steps, which are the instructions needed to carry out a policy statement.**

b. Procedures must be changed every 30 days.

c. Procedures are a prerequisite to developing a policy; they must exist before you can write a policy.

d. Procedures are suggestions for the best way to accomplish a certain task.

12- **In which of the following policy elements should the policy number appear?**

a. **Policy heading**

b. Policy statement of purpose

c. Policy objectives

d. Statement of authority

13- **Which of the following do the Graham-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) require in an organization's information security policy?**

a. The date the policy was written and revised

b. A schedule for future policy review and revision

c. A statement with consequences of violating the policy

d. **All of the above**

14- **Which of the following is true of policy elements?**

a. They are only standards, guidelines, and procedures

b. Policy elements are an optional component of a policy

c. Best practice dictates that all policy elements should be included in the policy document itself

d. They depend on, and support each other, while supporting the document as a whole

15- Which of the following is NOT one of the common pitfalls encountered when policy companions (standards, guidelines, and procedures) are combined into the same document as the policy itself?

a. Difficult to implement

b. Difficult to manage

c. Difficult to update

d. Difficult to justify

16- Which of the following questions is answered by the policy objective?

a. Why
b. How
c. What
d. When

17- Where would you find the name of your company and the effective date of the policy you're looking at?

a. Policy heading
b. Policy objectives
c. Policy statement of purpose
d. Statement of authority

18- Which of the following is an easy mistake, which should be avoided when preparing the policy statement of purpose?

a. Attempt to get too detailed

b. Forget to include the signature line

c. Omit the effective date of the policy

d. Describe in broad terms how the policy will be implemented

19- **Which of the following is NOT a way in which the policy definitions make the policy better?**

a. Policy definitions enable the target audience to better understand the policy

b. Policy definitions help to provide a legal baseline

c. **Policy definitions make the policy look like other official documents**

d. Policy definitions make the policy document more efficient

20- **The disciplinary process indicated in an information security policy enforcement clause usually includes which of the following most severe punishments?**

a. **Dismissal or criminal prosecution**

b. Loss of one month's pay

c. Demotion to a lower level

d. Transfer to another division in the company

21- **Which of the following is NOT something that a statement of authority tries to do?**

a. Explain the organization's reason for writing the documents

b. Recruit readers and show what is expected of them as employees

c. **Define what employees are expected to do in order to comply with the policies**

d. Describe regulatory compliance responsibilities that the company has

22- **Which of the following documents is likely to change most often?**

a. **Guidelines, because new improved best practices continually emerge**

b. Standards, because they are specific to the technology platform in use

c. Procedures, because they are so detailed

d. Policies, because they reflect core values

23- **Which of the following most likely be in the policy exceptions part of a company's policy that prohibits the use of modems?**

a. **All requests for modems must be approved by the Information Security department prior to installation**

b. A modem inventory form must be sent to the Information Security department immediately following the installation of all new modems

c. Only Bell 202C modems may be installed

d. No modems whatsoever may be installed

24- **Which of the following is MOST likely to reflect the policy audience for a corporate ethics policy at Acme Manufacturing?**

a. All Acme Manufacturing employees, and all vendors and service providers

b. All full- and part-time employees of Acme Manufacturing and its subsidiaries

c. The Acme Manufacturing Board of Directors

d. The Finance, Human Resources, and Marketing departments of Acme Manufacturing

25- **Which of the following is contained in the policy statement?**

a. The rules for implementing the policy

b. The location of documents that explain the reasoning behind the rules

c. Sometimes the step-by-step procedures required to perform the tasks defined in the policy

d. All of the above

26- **If a new United States federal information-sharing law is adopted, which of the following best represents a related information security policy statement of purpose?**

a. Uphold the U.S. Constitution

b. Ensure compliance with federal law

c. Prevent personal information from being used for identity theft

d. Maintain individuals' right to privacy, as granted under the U.S. Constitution

27- **If a new United States federal information-sharing law is adopted, which of the following best represents a related information security policy objective?**

a. Ensure compliance with federal law

b. Obtain prior written approval from all individuals whose personal data is to be shared

c. Maintain individuals' right to privacy, as granted under the U.S. Constitution

d. Prevent personal information from being used for identity theft

28- **Which of the following best describes the sequence of action steps posted on the front of an**

automated teller machine (ATM) at a bank?

a. Standards
b. **Procedures**
c. Guidelines
d. Policies

29- **Which of the following best describes Guidelines?**

a. Demands
b. **Suggestions**
c. Questions
d. Statements

30- **If a policy refers the reader to another section for clarification of any instance of non-standard language, that other section would best be called which of the following?**

a. **Policy Definitions**
b. Policy Header
c. Policy Enforcement Clause
d. Policy Exceptions

31- **Which of the following best describes how the penalties defined in the Policy Enforcement Clause should relate to the infractions?**

a. Any infraction should result in suspension or termination

b. The same penalty should apply each time an infraction occurs

c. **The penalty should be proportional to the level of risk incurred as a result of the infraction**

d. Penalties should be at the discretion of management

32- **Which of the following best describes how policy exception requests should be handled?**

a. Requestors should only be notified after their exception requests are approved

b. **Requestors should always receive a response to any request, whether approved or not**

c. Requestors should be notified why their exception requests were denied, so they can do a better job the next time

d. Requestors should be able to count on a seven-day turnaround on any policy exception request

33- **Which of the following describes how much of the final policy document is typically made up of policy statements?**

a. The policy statement is one section of the final policy document

b. Policy statements appear throughout the final policy document

c. Policy statements typically represent about 45% of the final policy document

d. **The bulk of the final policy document is composed of policy statements**

34- **Which of the following best describes when the policy audience is most likely to include people outside the organization?**

a. **The policy audience needs to include people outside the organization whenever those people are involved with an aspect of the organization or its information**

b. Any policy audience generally includes people outside the organization, because companies depend so heavily on outsourcing these days

c. People outside the organization should not be part of the policy audience, because there is no way to apply the policy enforcement clause against them

d. This is spelled out in the non-disclosure agreement

35- Which of the following best represents a Policy Statement of Purpose for a credit card company's Graham-Leach-Bliley Act compliance policy?

a. **Comply with federal law, by mailing annual disclosures to customers**

b. Mail annual disclosures to customers, and conduct annual training for employees

c. Comply with federal law, in order to protect the company's reputation

d. Protect customers' personal information

36- **Which of the following parts of an organization's software policy would most likely indicate that any new software purchases be made only from the approved software products list?**

a. Policy statement of purpose

b. Policy exceptions

c. **Policy objective**

d. Policy audience

37- **Which of the following is the MOST important rule of thumb to follow when developing the policy heading?**

a. The policy number must be included in the policy heading

b. **Ensure its structure is scalable, so that it is able to accommodate changes in the future, without losing its original organization**

c. Plan to spend the most time working on the policy heading; it is the most important part of the document

d. Ensure the policy heading contains all the same information as every other policy

38- **Which of the following is true of the Statement of Authority?**

a. **It is usually not found in each individual policy, and serves as a preface to a group of policies and the entire information security program**

b. It should strike fear into the hearts of all readers, in order to get them to take the policy seriously

c. It should contain very strict language, in order to impress people with its importance

d. It must appear in each individual policy, because it explains the company's motivation for developing the policies

39- **In which of the following ways does understanding policy elements help you interpret your organization's information security policies?**

a. Awareness of policy elements helps you determine the strength of the policy, and whether you should take it seriously

b. If you understand policy elements, you will be able to change the policies

c. **Knowing the purpose and goal of each section of the policy can help you better understand the intent of the policy, as well as how the policy applies to you**

d. You need to know the policy elements in order to determine which parts of the policy apply to you

40- **If you are assigned to author your company's information security policies, which of the following is the MOST important thing to do first?**

a. Look at all the other policies to get an idea of how they are written

b. **Plan before you write**

c. Determine when they are due

d. Express thanks for being given such a good assignment

41- **The setup instructions that come in the box when you buy a new printer are an example of which of the following?**

a. Standards
b. Procedures
c. Guidelines
d. Policies

42- **The passage "In order to protect their home computers, remote users should consider installing anti-virus software, a firewall, and anti-spam filters" represents which of the following:**

a. Procedures
b. Guidelines
c. Policy
d. Standards

43- **In which of the following ways do password construction standards in a password policy make it better?**

a. Standards suggest options for the best way to comply with the policy

b. Standards provide a permanent basis for the policy

c. Standards help to ensure consistency with minimum requirements

d. Standards indicate who is affected by the policy

44- **Which of the following is a good way to help ensure that your company's information security policies represent best practices?**

a. Base them on current industry standards for practices and technology

b. Provide little or no opportunity for policy exceptions to be granted

c. Copy key parts of similar policies you find on the Internet

d. Keep the suggested guidelines to a minimum, and focus on mandatory standards

45- **When writing a new information security policy to cover data movement within your company, which of the following represents the BEST approach to take in order to ensure the policy will fulfill its intended purpose, help the policy audience understand what they need to do, and be sustainable?**

a. Provide supporting documentation outside the policy document, in order to make it easier to implement, manage, and update

b. Follow existing standards, guidelines, and procedures as the policy

c. Develop a comprehensive policy, by including all applicable policy elements and

supporting documentation in the policy document

d. Hold workshops to build employees' awareness of the policy after it is written and approved

46- **Which of the following is the reason why United States government official communications about new federal laws frequently include references to other documents?**

a. This approach is required by law

b. Congress must ensure that the new laws are comprehensive, so they can be defended in court

c. **These references help those affected by the new laws gain a better understanding of what they need to do**

d. It makes it easier to keep track of things

47- **In which of the following ways does understanding policy elements enable the development of information security policies?**

a. One cannot develop information security policies without an understanding of policy elements

b. **Understanding policy elements enables us to break the policies down into their essential components, in order to more efficiently and effectively create usable policies**

c. Information security policies must include all policy elements in order to be valid

d. It is necessary to understand policy elements in order to document which penalties apply for violation of information security policies

48- **Which of the following is NOT true of policy elements?**

a. Policy elements can be thought of as individual sections of the policy document

b. **Standards, guidelines, and procedures are policy elements**

c. Each policy element has its own specific purpose

d. Understanding policy elements helps you focus on the goal of each section of the policy, in order to be more consistent in how you write

49- **Which of the following is an important function of the statement of authority?**

a. **It provides a bridge between an organization's core values and security strategies**

b. It indicates who to talk to if you want to request a change in the policy

c. It describes the penalties for policy infractions

d. It references standards, guidelines, and procedures which the reader can consult for clarification of the policy

50- Which of the following is a reason why information security policy documents should include a version or change control number?

a. **In order to maintain consistency**

b. It is required by law

c. It can be a good way to promote that you wrote the policy

d. Information technology uses a lot of math

Fill in the Blank:

51- The _____ is the part of the document that is traditionally the one that constitutes the bulk of the final document known as the policy.

Answer: policy statement

52- The _____ states the goal of the policy, or what we are trying to achieve by implementing the policy.

Answer: policy objective

53- A _____ suggests the best way to accomplish a certain task.

Answer: guideline

54- The _____ allows the organization to assert the seriousness of the policy.

Answer: Policy Enforcement Clause

55- Policy companions include specific standards, suggested _____, and sequential procedures.

Answer: guidelines

Matching:

56- Match each part of the policy statement with what it defines:

I. goal	A. why
II. audience	B. what
III. purpose	C. who

Answer: B C A

57- Match each of the following terms to its respective part of the policy excerpt that appears below:

"Fair business practices are a cornerstone of our company's corporate ethics program. In support of this goal, Acme Manufacturing will require all employees to decline all gifts or entertainment offered to them by vendors, and to report all offers to the Ethics Office. The purpose of this policy is to maintain the company's business ethics by clearly informing all employees of their obligations to be ethical in their business dealings on behalf of the company."

I. What	A. Clearly inform all employees of their obligations
II. Why	B. All employees
III. How	C. Decline all offers of gifts or entertainment, and report all offers
IV. Who	D. Maintain the company's business ethics

Answer: C D A B

Match the terms below to complete each cliché that applies to the policy enforcement clause:

I. add	A. the language
II. walk	B. some muscle
III. live	C. some bite to your bark
IV. do	D. your talk
V. flex	E. what you say

Answer: C D A E B

CHAPTER 3: INFORMATION SECURITY FRAMEWORK

Multiple Choice:

1. **What does CIA stand for?**

VVVV. Confidentiality, Integrity and Authorization

WWWW. Confidentiality, Integrity and Accountability

XXXX. Confidentiality, Integrity and Authentication

YYYY. Confidentiality, Integrity and Availability

1. **The goal of protecting confidentiality is to:**

ZZZZ. Prevent the unauthorized disclosure of sensitive information

AAAAA. Prevent the authorized disclosure of sensitive information

BBBBB. Prevent the unauthorized disclosure of public information

CCCCC. Prevent the authorized disclosure of public information.

DDDDD. Which of the following is NOT a threat to data confidentiality?

EEEEE. Hackers

FFFFF. Encryption

GGGGG. Improper access controls

HHHHH. Social engineering

IIIII. What is shoulder surfing?

JJJJJ. Conning someone into giving away their password

KKKKK. Looking at a person using their computer in hopes of viewing sensitive information

LLLLL. Another word for social engineering

MMMMM. Waiting for a user to leave their workstation and taking their place behind the keyboard

Reference: "C" is for Confidentiality

NNNNN. Which of the following is NOT an example of social engineering?

OOOOO. Calling an employee on the phone and impersonating an IT consultant to learn passwords

PPPPP. Running a password-cracking utility against a web server

QQQQQ. Dressing up as UPS employee and gaining access to sensitive areas of a business

RRRRR. Posing as a potential customer in a Bank and gaining access to a computer terminal by pretending to need to send an email

Reference: "C" is for Confidentiality

SSSSS. Which of the following is NOT an example of malicious code?

TTTTT. Key logger

UUUUU. Virus

VVVVV. Worm

WWWWW. Solitaire

Reference: "C" is for Confidentiality

XXXXX. What is a valid definition of data integrity?

YYYYY. Knowing that the data on the screen is un-tampered with data

ZZZZZ. Data that is encrypted

AAAAAA. Data that has not been accessed by unauthorized users

BBBBBB. The knowledge that the data is transmitted in ciphertext only

CCCCCC. **Data integrity is**

DDDDDD. Protecting the data from intentional or accidental disclosure

EEEEEE. Making sure the data is always available when legitimately needed

FFFFFF. Protecting the data from intentional or accidental modification

GGGGGG. Making sure the data is always transmitted in encrypted format

HHHHHH. An employee accidentally makes changes to a company-owned file. This is known as a violation of:

IIIIII. Data Confidentiality

JJJJJJ. Data Integrity

KKKKKK. Data Availability

LLLLLL. Dave Authorization

MMMMMM. Which of the following is NOT a threat to data integrity?

NNNNNN. Hackers

OOOOOO. Improper access controls

PPPPPP. Use of encrypted emails

QQQQQQ. Malicious code

RRRRRR. Data availability is the assurance that:

SSSSSS. Only authorized users will gain access to a resource

TTTTTT. All data stored on a hard drive is encrypted

UUUUUU. All sensitive data stored on a hard drive is encrypted

VVVVVV. Data and systems are accessible anytime they are needed

Reference: "A" is for Availability

WWWWWW. Guaranteed 99.999% uptime is an example of:

XXXXXX. Data integrity

YYYYYY. Data authentication

ZZZZZZ. Data confidentiality

AAAAAAA. Data availability

Reference: "A" is for Availability

Fill in the Blank:

BBBBBBB. Availability is the assurance that systems and data are _____ by authorized users when needed.

Answer: accessible

CCCCCCC. The _____ agreement is a type of agreement between the service provider and a customer.

Answer: service level

DDDDDDD. Networks are more vulnerable to _____ threats than to the other components of the CIA triad.

Answer: availability

EEEEEEE. The positive identification of the person or system seeking access is known as _____.

Answer: authentication

FFFFFFF. Granting users and systems a predetermined level of access to information resources is known as _____.

Answer: authorization

GGGGGGG. The logging of access and usage of information resources is known as _____.

Answer: accounting

IT 409

Matching:

HHHHHHH. Match each topic with its definition to the right:

I.	Accountability	A. The logging of access and usage of information resources
II.	Assurance	B. The process of tracing actions to their source
III.	Authentication	C. The processes used to develop confidence that security measures are working
IV.	Authorization	D. The positive identification of the person or system seeking access
V.	Accounting	E. Granting users a predetermined level of access to information resources

Answer: B C D E A

IIIIIII. Match the following terms to their meanings:

I.	Confidential	A. Information available internally on a need to know basis
II.	Sensitive	B. Information meant to be kept secret & restricted to a small circle of authorized
III.	Public	C. Disclosure of this data would have no implication for the company

Answer: B A C

JJJJJJJ. Match the following terms to their meanings:

I.	Information ownership	A. Charged to those liable & responsible for protecting the information
II.	Information custodians	B. Individuals with original responsibility for polices and practices
III.	Information owners	C. Those charged with maintaining the systems that store, process and transmit information

Answer: A C B

KKKKKKK.

IT 409

Match the following terms to their meanings:

I. MAC A. Classification system used by the federal government and the military

II. RBAC B. Classification system where the owner decides who gets what level of access

III. DAC C. Classification system that uses the employee's role to grant authorization

Answer: A C B

LLLLLLL. Match the following ISO 17799:2000 domains to their definition:

I. Security Policy A. Design and maintenance of a secure environment to prevent damage and unauthorized access to the business premises

II. Organizational Security B. Provides direction and support for the information security program

III. Asset Classification and Control C. Involves creating an inventory of all data and data systems

IV. Personnel Security D. Establish and support a management framework for information security

V. Physical and Environmental Security E. Implement controls for secure hiring and termination of staff

Answer: B D C E A

MMMMMMM. Match the following ISO 17799:2000 domains to their definition:

I. Access Control A. To ensure that the organization's information systems conform to local, national and international laws and mandates

II. Compliance B. To prevent unauthorized access to data or information systems

III. Business Continuity Management C. Provide security guidelines for creation of secure code and applications

IV. System Development & Maintenance D. To protect the company from any situation that would result in the company not being able to perform its business tasks

V. Communications & Operations Management E. To ensure the correct and secure operation of information processing facilities

Answer: B A D C E

CHAPTER 4: SECURITY POLICY DOCUMENTS AND ORGANIZATIONAL SECURITY POLICIES

Multiple Choice:

1. **Who should issue the statement of authority?**

NNNNNNN. The IT Manager

OOOOOOO. All the information owners

PPPPPPP. All the employees

QQQQQQQ. **The CEO, President or Chairman of the Board**

1. **This policy document is used to convey the organization's intention, objective, and commitment. It is known as:**

RRRRRRR. **The statement of authority**

SSSSSSS. The Acceptable Use Policy

TTTTTTT. The affirmation agreement

UUUUUUU. The service level agreement

VVVVVVV. **The statement of authority is also a statement of:**

WWWWWWW. Controls

XXXXXXX. **Culture**

YYYYYYY. Do's and Don'ts

ZZZZZZZ. Operations

AAAAAAAA.

This policy document is often referred to as a "policy about a policy". What is its real name?

BBBBBBBB. Service level agreement

CCCCCCCC. Security Policy Document Policy

DDDDDDDD. Statement of authority

EEEEEEEE. Acceptable use policy

FFFFFFFF. Which of the following is NOT contained in the Security Policy Document Policy?

GGGGGGGG. Who is in charge of designing the policy

HHHHHHHH. What users may or may not do

IIIIIIII. Who is in charge of enforcing the policy

JJJJJJJJ. A statement about the need for information security policies

KKKKKKKK. What is an "employee version" of the security policies?

LLLLLLLL. A version written without the help of management

MMMMMMMM. A version that does not contain the affirmation agreement

NNNNNNNN. A version that does not contain the acceptable use policy

OOOOOOOO. A succinct version of the comprehensive policy document that only includes information that pertains to the entire user base

PPPPPPPP. The ISO Standard known as Managing Organizational Security includes several categories. Which of the following is NOT one of them?

QQQQQQQQ. Organizational Security Controls

RRRRRRRR. Information Security Infrastructure

SSSSSSSS. Identification of Risks from Third Parties

TTTTTTTT. Security Requirements for Outsourcing

UUUUUUUU.

Which of the following federal regulations pertains to the medical field?

VVVVVVVV. FERPA

WWWWWWWW. GLBA

XXXXXXXX. HIPAA

YYYYYYYY. SOX

ZZZZZZZZ. Which of the following federal regulations pertains to the educational field?

AAAAAAAA. FERPA

BBBBBBBB. GLBA

CCCCCCCC. HIPAA

DDDDDDDD. SOX

EEEEEEEE. As it pertains to information security policies, what is the SOA?

FFFFFFFF. Start of authority

GGGGGGGG. Statement of Accountability

HHHHHHHH. Statement of Authority

IIIIIIII. Summary of Authentication

Fill in the Blank:

JJJJJJJJ. For a security policy to be successful, there must be a _____ from leadership.

Answer: commitment

KKKKKKKK. The _____ is an introduction to the overall information security policy.

Answer: statement of authority

LLLLLLLL. The goal of the statement of authority is to deliver a _____ about the importance of information security to all who read the document.

Answer: clear message

MMMMMMMM. Creating a _____ of security requires positive influences at multiple levels within the organization.

Answer: culture

NNNNNNNNN. _____ reinforce by example the message that security practices are important to the organization.

Answer: Security champions

OOOOOOOOO. _____ are events within an organization that affect culture, procedures, activities, employee responsibilities, and relationships. They should trigger risks and vulnerability assessments.

Answer: Change drivers

PPPPPPPPP. When outsourcing work, pre-engagement _____ investigations and clearly stated contractual obligations are extremely important

Answer: due diligence

QQQQQQQQQ. Acceptable use agreements are often called _____

Answer: Employee Affirmation

Matching:

RRRRRRRRR. Match the following federal regulations to their target audience:

I. HIPAA	A. Educational Institutions
II. SOX	B. Healthcare service providers
III. FERPA	C. Financial institutions
IV. GLBA	D. Publicly traded companies

Answer: B D A C

SSSSSSSSS. Match the following terms to their meanings:

I. Change driver	A. Introduction to the policy document
II. Acceptable use agreement	B. Policy about a policy
III. Statement of authority	C. any event that impacts culture, procedures and activities within an organization
IV. Security Policy Document Policy	D. List of actions that employees are not allowed to perform while using company-provided equipment

Answer: C D A B

CHAPTER 5: ASSET CLASSIFICATION

Multiple Choice:

1. **Which section of the ISO 17799 deals with asset classification?**

TTTTTTTTT. 2
UUUUUUUUU. 3
VVVVVVVVV. 4
WWWWWWWWW. 5

1. **Which of the following provide a way and place to process, store, transmit, and communicate information?**

XXXXXXXXX. Information systems

YYYYYYYYY. Information assets

ZZZZZZZZZ. Off-site storage solutions

AAAAAAAAAA. Outsourced storage solutions

BBBBBBBBBB. Information systems are a combination of

CCCCCCCCCC. applications

DDDDDDDDDD. hardware and software

EEEEEEEEEE. controls and procedures

FFFFFFFFFF. policies and procedures

GGGGGGGGGG. **This classification level is used by the military for items "the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to National Security":**

HHHHHHHHHH. For your eyes only

IIIIIIIIII. Top Secret

JJJJJJJJJ. Secret

KKKKKKKKKK. Confidential

LLLLLLLLLL. This classification level is used by the military for items "the unauthorized disclosure of which reasonably could be expected to cause serious damage to National Security":

MMMMMMMMMM. For your eyes only
NNNNNNNNNN. Top Secret
OOOOOOOOOO. Secret
PPPPPPPPPP. Confidential

QQQQQQQQQ. **This classification level is used by the military for items "the unauthorized disclosure of which reasonably could be expected to cause damage to National Security":**

RRRRRRRRRR. For your eyes only
SSSSSSSSSS. Top Secret
TTTTTTTTTT. Secret
UUUUUUUUUU. Confidential

@. Which of the following is NOT a step used by hackers to infiltrate a network?

A. Footprinting
B. Data corruption
C. scanning
D. enumeration

E. Which data classification method is used by the US military?

F. DAC
G. RBAC
H. RDAC
I. MAC

J. When it comes to information security, what is labeling the vehicle for?

K. Communicating the sensitivity level
L. Communicating the access controls
M. Enforcing the access controls
N. Auditing the access controls

O. Information labels should be:

P. encrypted
Q. hidden
R. universally understandable
S. symbol-based only

T. Information needs to be handled according to:

U. **Its classification level**

V. The statement of authority

W. The access controls set forth in the asset management policy

X. The access controls set forth in the affirmation agreement

Y. **Who is directly responsible for defining information asset protection?**

Z. The CEO/President/Chairman of the Board

AA. The ISO

BB. **The Information Owner**

CC. The Information Custodian

DD. **Who is directly responsible for implementing information asset protection controls?**

EE. The CEO/President/Chairman of the Board
FF. The ISO
GG. The Information Owner
HH. The Information Custodian

II. **Who is directly responsible for using information asset in accordance with their classification levels?**

JJ. The users
KK. The ISO
LL. The Information Owner
MM. The Information Custodian

NN. **This is known as the process of upgrading the classification level of an information asset:**

OO. Declassification
PP. Classification review
QQ. Reclassification
RR. Classification Upgrade

SS. This is known as the process of downgrading the classification level of an information asset:

TT. **Declassification**

UU. Classification review

VV. Reclassification

WW. Asset Publication

XX. When calculating the value of an asset, which of the following is NOT a criterion?

YY. Cost to acquire or develop asset

ZZ. Cost to maintain and protect the asset

AAA. Cost to disclose the asset

BBB. Reputation

CCC. Hardware assets are:

DDD. programs

EEE. code snippets

FFF. tangible pieces of equipment

GGG. Operating system

HHH. Which of the following is NOT an example of a software asset?

III. programs

JJJ. code

KKK. wireless access point

LLL. Operating system

Fill in the Blank:

MMM. Each asset, whether software or hardware, should have a _____.

Answer: unique identifier

NNN. Best practices dictate that the organization chooses a naming _____ for its assets and apply the standard consistently

Answer: convention

OOO. An asset _____ should illustrate what an asset is used for.

Answer: description

PPP. For hardware devices, the manufacturer-assigned _____ should be recorded.

Answer: serial number

QQQ. The _____ address refers to the geographic location of the device itself, or the device that houses the information.

Answer: physical

RRR. The _____ address is where the asset can be found on the organization's network.

Answer: logical

SSS. The controlling _____ is the department or business what purchased or paid for the asset.

Answer: entity

TTT. Criticality _____ provide a company with the basis on which to prioritize and allocate resources.

Answer: ratings

UUU. An information classification program _____ starts with assigning classification levels and ends with the process of declassification.

Answer: lifecycle

VVV. An information classification procedure is to characterize the _____ of the information system.

Answer: criticality

WWW. If the classification level of an asset must be upgraded, it is a process known as _____ .

Answer: reclassification

XXX. A(n) _____ is a definable piece of information, stored in any manner, which is recognized as having a value to the organization.

Answer: information asset

YYY. The first step to protecting assets is to create an asset _____ .

Answer: inventory

ZZZ. _____ refers to how vital this information asset is to business processes and/or customer service.

Answer: System impact

AAAA. _____ refers to the level of safeguards and/or controls required to protect the asset.

Answer: Protection level

Matching:

BBBB. Match each concept with its definition:

I. Information Labeling A. Information needs to be used in accordance with its classification

II. Familiar labels B. The vehicle for communicating the sensitivity level

III. Information handling C. Classification labels should be easily understandable

Answer: B C A

CCCC. Commercial asset classification model: match the level with the definition:

I. Confidential A. business-centric information to be used internally only

II. Sensitive B. Meant to be kept secret and restricted to only a small circle of employees

III. Restricted C. information that does not require protection

IV. Public D. Sometimes referred to as “personal” or “privileged”

Answer: B D A C

DDDD. Match the following hacking steps to their meanings:

I. footprinting A. gathering specific network data such as user names and shares

II. scanning B. launching an exploit

III. enumerating C. process of accumulating data regarding a specific logical or physical target

IV. attacking D. process of identifying vulnerabilities on a target network/host

Answer: C D A B

EEEE. Commercial asset classification model: match the level with the definition.

I. Top Secret A. disclosure could cause serious damage to National Security

II. Secret B. disclosure could cause exceptionally grave damage to National Security

III. Confidential C. disclosure would cause no damage to National Security

IV. Unclassified D. disclosure could cause damage to National Security

Answer: B A D C

FFFF. Match the assets with their corresponding examples:

I. Databases A. Drawings, schematics, patents

II. Data files B. Information about customers, personnel, and/or finances

III. Intellectual Property C. Detailed instructions on how to perform various activities

IV. Research documentation D. Transactional data giving up-to-date information about each event

V. Operational procedures E. Proprietary information based on experimentation

Answer: B D A E C

CHAPTER 5: ASSET CLASSIFICATION

Multiple Choice:

1. **Which section of the ISO 17799 deals with asset classification?**

GGGG. 2

HHHH. 3

IIII. 4

JJJJ. 5

KKKK. Which of the following provide a way and place to process, store, transmit, and

communicate information?

LLLL. Information systems

MMMM. Information assets

NNNN. Off-site storage solutions

OOOO. Outsourced storage solutions

PPPP. Information systems are a combination of:

QQQQ. applications

RRRR. hardware and software

SSSS. controls and procedures

TTTT. policies and procedures

UUUU. This classification level is used by the military for items "the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to National Security":

VVVV. For your eyes only

WWWW. Top Secret

XXXX. Secret

YYYY. Confidential

ZZZZ. This classification level is used by the military for items "the unauthorized disclosure of which reasonably could be expected to cause serious damage to National Security":

AAAAA. For your eyes only

BBBBB. Top Secret

CCCCC. Secret

DDDDD. Confidential

EEEEE. This classification level is used by the military for items "the unauthorized disclosure of which reasonably could be expected to cause damage to National Security":

FFFFF. For your eyes only

GGGGG. Top Secret

HHHHH. Secret

IIIII. Confidential

JJJJJ. Which of the following is NOT a step used by hackers to infiltrate a network?

KKKKK. Footprinting

LLLLL. Data corruption

MMMMM. scanning

NNNNN. enumeration

OOOOO. Which data classification method is used by the US military?

PPPPP. DAC

QQQQQ. RBAC

RRRRR. RDAC

SSSSS. MAC

TTTTT. When it comes to information security, what is labeling the vehicle for?

UUUUU. Communicating the sensitivity level

VVVVV. Communicating the access controls

WWWWW. Enforcing the access controls

XXXXX. Auditing the access controls

YYYYY. Information labels should be:

ZZZZZ. encrypted

AAAAAA. hidden

BBBBBB. universally understandable

CCCCCC. symbol-based only

DDDDDD. Information needs to be handled according to:

EEEEEE. Its classification level

FFFFFF. The statement of authority

GGGGGG. The access controls set forth in the asset management policy

HHHHHH. The access controls set forth in the affirmation agreement

IIIIII. Who is directly responsible for defining information asset protection?

JJJJJJ. The CEO/President/Chairman of the Board

KKKKKK. The ISO

LLLLLL. The Information Owner

MMMMMM. The Information Custodian

NNNNNN. Who is directly responsible for implementing information asset protection controls?

OOOOOO. The CEO/President/Chairman of the Board

PPPPPP. The ISO

QQQQQQ. The Information Owner

RRRRRR. The Information Custodian

SSSSSS. Who is directly responsible for using information asset in accordance with their classification levels?

TTTTTT. The users

UUUUUU. The ISO

VVVVVV. The Information Owner

WWWWWW. The Information Custodian

XXXXXX. This is known as the process of upgrading the classification level of an information asset:

YYYYYY. Declassification

ZZZZZZ. Classification review

AAAAAAA. Reclassification

BBBBBBB. Classification Upgrade

CCCCCCC. This is known as the process of downgrading the classification level of an information asset:

DDDDDDD. Declassification

EEEEEEE. Classification review

FFFFFFF. Reclassification

GGGGGGG. Asset Publication

HHHHHHH. When calculating the value of an asset, which of the following is NOT a criterion?

IIIIIII. Cost to acquire or develop asset

JJJJJJJ. Cost to maintain and protect the asset

KKKKKKK. Cost to disclose the asset

LLLLLLL. Reputation

MMMMMMM. Hardware assets are:

NNNNNNN. programs
OOOOOOO. code snippets
PPPPPPP. tangible pieces of equipment
QQQQQQQ. Operating system

RRRRRRR. Which of the following is NOT an example of a software asset?

SSSSSSS. programs
TTTTTTT. code
UUUUUUU. wireless access point
VVVVVVV. Operating system

Fill in the Blank:

WWWWWWW. Each asset, whether software or hardware, should have a _____.

Answer: unique identifier

XXXXXXX. Best practices dictate that the organization chooses a naming _____ for its assets and apply the standard consistently

Answer: convention

YYYYYYY. An asset _____ should illustrate what an asset is used for.

Answer: description

ZZZZZZZ. For hardware devices, the manufacturer-assigned _____ should be recorded.

Answer: serial number

AAAAAAAA. The _____ address refers to the geographic location of the device itself, or the device that houses the information.

Answer: physical

BBBBBBBB. The _____ address is where the asset can be found on the organization's network.

Answer: logical

CCCCCCCC. The controlling _____ is the department or business what purchased or paid for the asset.

Answer: entity

DDDDDDDD. Criticality _____ provide a company with the basis on which to prioritize and allocate resources.

Answer: ratings

EEEEEEEE. An information classification program _____ starts with assigning classification levels and ends with the process of declassification.

Answer: lifecycle

FFFFFFFF. An information classification procedure is to characterize the _____ of the information system.

Answer: criticality

GGGGGGGG. If the classification level of an asset must be upgraded, it is a process known as _____ .

Answer: reclassification

HHHHHHHH. A(n) _____ is a definable piece of information, stored in any manner, which is recognized as having a value to the organization.

Answer: information asset **Reference:** What Are We Trying to Protect?

IIIIIIII. The first step to protecting assets is to create an asset _____ .

Answer: inventory **Reference:** What Are We Trying to Protect?

JJJJJJJJ. _____ refers to how vital this information asset is to business processes and/or customer service.

Answer: System impact

KKKKKKKK. _____ refers to the level of safeguards and/or controls required to protect the asset.

Answer: Protection level

Matching:

LLLLLLLL. Match each concept with its definition:

I. Information Labeling A. Information needs to be used in accordance with its classification

II. Familiar labels B. The vehicle for communicating the sensitivity level

III. Information handling C. Classification labels should be easily understandable

Answer: B C A

MMMMMMMM. Commercial asset classification model: match the level with the definition:

I. Confidential A. business-centric information to be used internally only

II. Sensitive B. Meant to be kept secret and restricted to only a small circle of employees

III. Restricted C. information that does not require protection

IV. Public D. Sometimes referred to as “personal” or “privileged”

Answer: B D A C

NNNNNNNN. Match the following hacking steps to their meanings:

I. footprinting A. gathering specific network data such as user names and shares

II. scanning B. launching an exploit

III. enumerating C. process of accumulating data regarding a specific logical or physical target

IV. attacking D. process of identifying vulnerabilities on a target network/host

Answer: C D A B

OOOOOOOO. Commercial asset classification model: match the level with the definition.

I. Top Secret A. disclosure could cause serious damage to National Security

II. Secret B. disclosure could cause exceptionally grave damage to National Security

III. Confidential C. disclosure would cause no damage to National Security

IV. Unclassified D. disclosure could cause damage to National Security

Answer: B A D C

PPPPPPPP. Match the assets with their corresponding examples:

I. Databases A. Drawings, schematics, patents

II. Data files B. Information about customers, personnel, and/or finances

III. Intellectual Property C. Detailed instructions on how to perform various activities

IV. Research documentation D. Transactional data giving up-to-date information about each event

V. Operational procedures E. Proprietary information based on experimentation

Answer: B D A E C

CHAPTER 6: PERSONNEL SECURITY

Multiple Choice:

1. **Which section of the ISO 17799 deals with personnel security?**

QQQQQQQQ. 3
RRRRRRRR. 4
SSSSSSSS. 5
TTTTTTTT. 6

IT 409

1. **A job description should NOT provide which of the following types of information?**

UUUUUUUU. The mission of the organization

VVVVVVVV. The responsibilities of the position

WWWWWWWW. Expectations regarding confidentiality

XXXXXXXX. Systems and software used for security

YYYYYYYY. The age group most inclined to use an online job search is:

ZZZZZZZZ. 30 to 49
AAAAAAAAA. 18 to 29
BBBBBBBBB. 50 to 64
CCCCCCCCC. 33% of persons across all age groups use online job searching

DDDDDDDDD. A security clearance investigation does NOT involve research into a person's:

EEEEEEEEE. character
FFFFFFFFF. reliability
GGGGGGGGG. family connections
HHHHHHHHH. trustworthiness

IIIIIIIII. Which of the following are types of background checks?

JJJJJJJJJ. credit history
KKKKKKKKK. criminal history
LLLLLLLLL. license verification
MMMMMMMMM. all of the above

NNNNNNNNN. Which of the following information about a person cannot be used to influence a hiring decision?

OOOOOOOOO. educational credentials
PPPPPPPPP. filing of a Workers' Compensation claim
QQQQQQQQQ. negative credit history
RRRRRRRRR. relevant certifications

SSSSSSSSS. Which of the following is a component of an affirmation agreement?

TTTTTTTTT. statement of authority
UUUUUUUUU. background check

VVVVVVVVV. job description
WWWWWWWWW. credit history

XXXXXXXXX. Which of the following is NOT a type of employee agreement?

YYYYYYYYY. acceptable use agreement
ZZZZZZZZZ. employee information security affirmation agreement
AAAAAAAAAA. certification maintenance agreement
BBBBBBBBBB. confidentiality agreement

CCCCCCCCCC. Which of the following are components of a good security incident reporting program?

DDDDDDDDDD. training users to recognize suspicious incidents
EEEEEEEEEE. providing follow-through and feedback
FFFFFFFFFF. establishing a system for reporting incidents
GGGGGGGGGG. all of the above

HHHHHHHHHH. An information security affirmation agreement would be likely to cover the use of

IIIIIIIIII. e-mail
JJJJJJJJJJ. office supplies
KKKKKKKKKK. parking
LLLLLLLLLL. paid time off

Fill in the Blank:

MMMMMMMMMM. Overly informative job postings provide information that may be used in _____ attacks.

Answer: social engineering

NNNNNNNNNN. A(n) _____ should never be allowed to tour the facility.

Answer: job candidate

OOOOOOOOOO. The organization of information assets according to their sensitivity to disclosure is called _____.

Answer: information classification

PPPPPPPPPP. _____ is the ranking of information assets in terms of their importance.

Answer: criticality

QQQQQQQQQQ. The government assigns a _____ to its personnel based on preset criteria and a background check.

Answer: clearance level **Reference:** Who Is This Person?

RRRRRRRRRR. Confidentiality agreements help to protect _____ rights.

Answer: patent

SSSSSSSSSS. An event that threatens information or an information system is called a(n) _____.

Answer: security incident

TTTTTTTTTT. A(n) _____ simply covers the rules for the proper use of information systems.

Answer: acceptable use agreement \

Matching:

UUUUUUUUUU. Match each type of employee agreement with its description:

I. Confidentiality agreement A. Teaches the importance of security and instills organizational values

II. Acceptable use agreement B. Protects against unauthorized disclosure of information

III. Employee information security affirmation agreement C. Focuses on proper use of information systems

Answer: B C A

@. Match the following terms with their relationship to personnel security:

I. Job description A. Scrutiny before hiring

II. Interview B. Reaches a wide audience of potential intruders

III. Background check C. May unintentionally provide too much information

IV. Employee agreement D. Establishes definitions for handling information

Answer: B C A D

IT 409

A. Match each of the following with its example:

I. Security education A. posters reminding users to report security breaches

II. Security training B. a presentation on creating good passwords

III. Security awareness C. recertification training for the network administrator

Answer: C B A